VISIT…

Lock Picking

Michael Lee

Math 187

Spring 2004

Lock Picking and Cryptanalysis

Cryptanalysis is the study of techniques that facilitate the deciphering of cryptographic code. Lock picking is a very similar science with the primary difference lying in the fact that while the bulk of cryptanalysis takes place in an indefinable place, lock picking is a physical activity and is done by feel. Aside from this basic difference, both of these arts are based upon the same principal, overcoming an obstacle that is in between you and something you are trying to access.

Lock Picking

Object in physical world

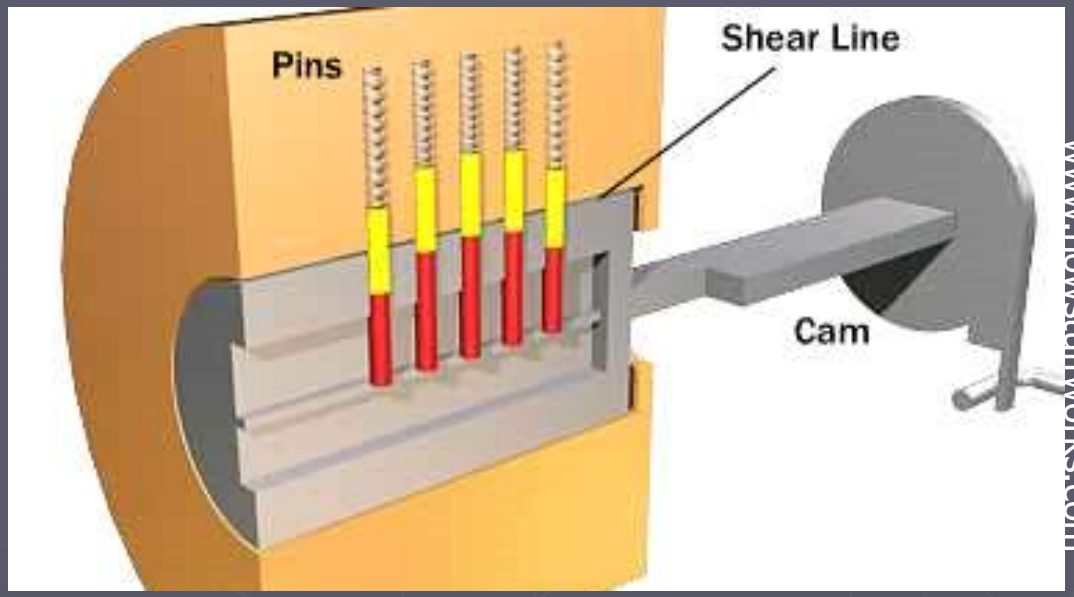
- Lock on object (door, safe, padlock, etc.)
- Key to the lock
- Item(s) you are attempting to acquire/gaining entry to an area

Cryptanalysis

Equivalent object in Cryptanalysis

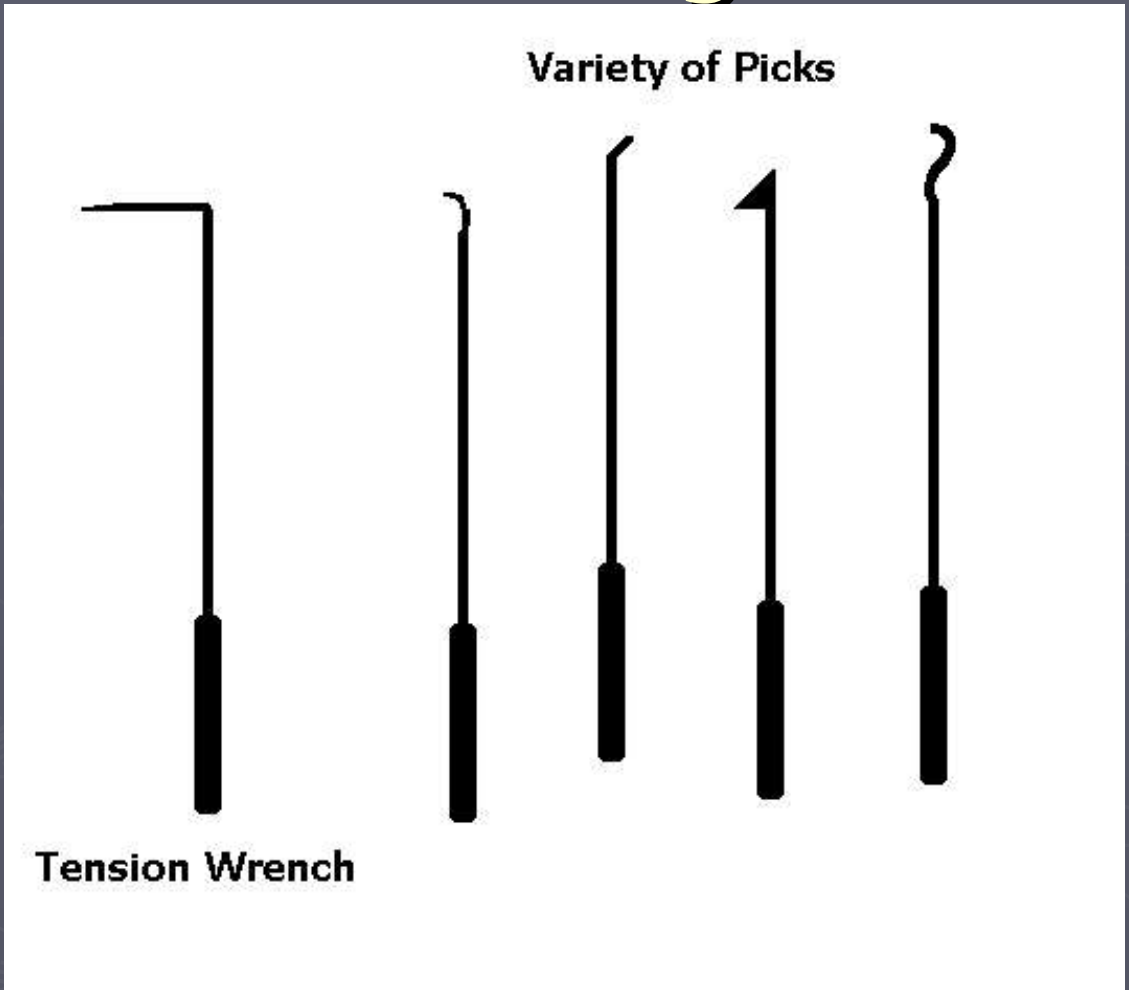
- Unbroken cipher text
- Key to the cryptographic system used
- The message in plaintext

How a Lock Works



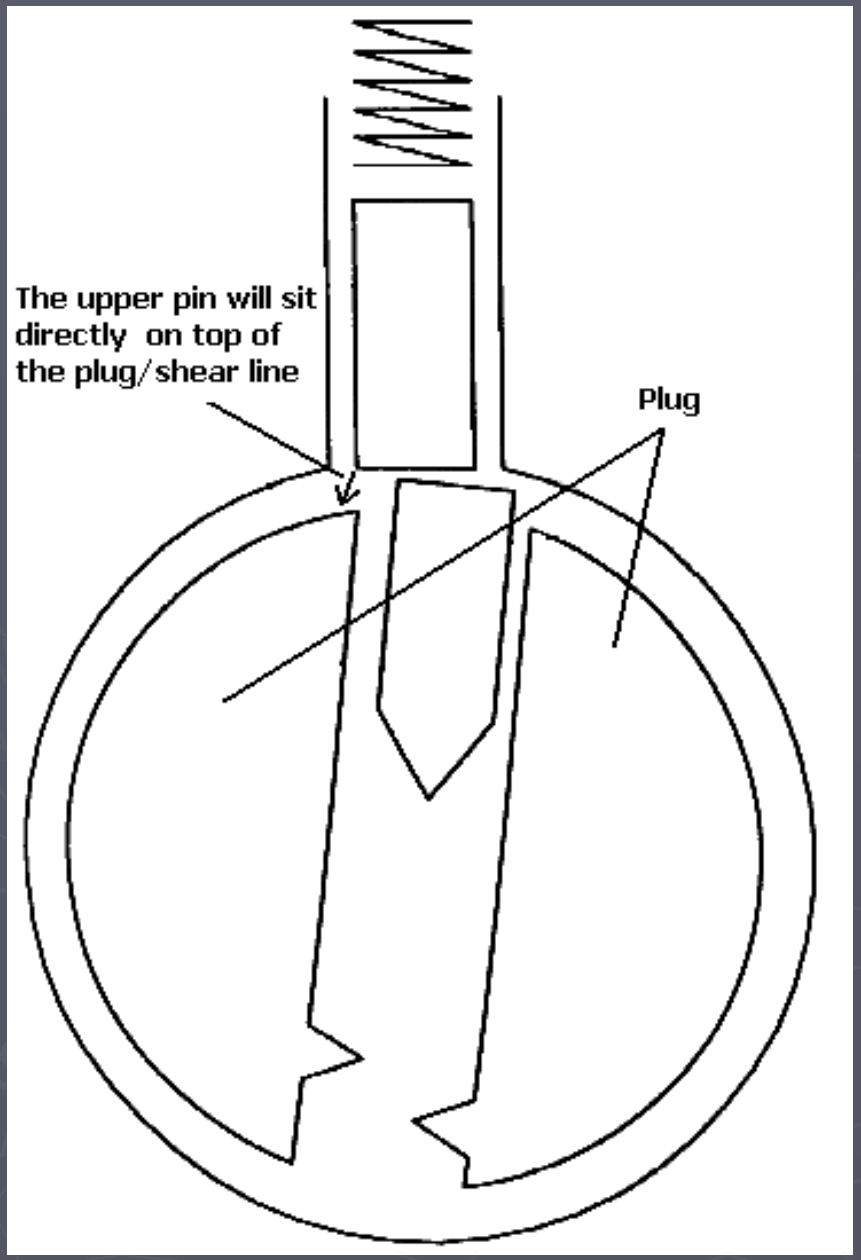
A majority of locks are of the style pictured above, known as cylinder locks. As any key is inserted into the keyhole the **pins** (denoted in both red and yellow) are pressed upon by the key and in turn compress the springs. If the correct key is used, each of the springs will compress just enough to allow the yellow and red portions of the pin to straddle the **shear line**. Since they are simply laying upon each other, when this occurs the **cam** is able to turn freely and the lock can be opened.

Lock Picking Tools



- Picks are used to lift individual pins
- Tension Wrenches are used for attempting to turn the cam, or, in other words create tension.

Picking a Lock



Taken and modified from www.capricorn.org

1. Insert tension wrench into the key hole. Apply torque in the same direction that you would turn the key. Doing this creates a "shelf" which the pins will in turn rest upon.
2. Insert a pick into the keyhole and begin prodding around in the plug shafts while attempting to press the pins upward. The goal here is to press each pair of pins until you hear a "click." If you are providing enough torque the uppermost pin will sit on the shelf in the housing.

Picking a Lock Continued

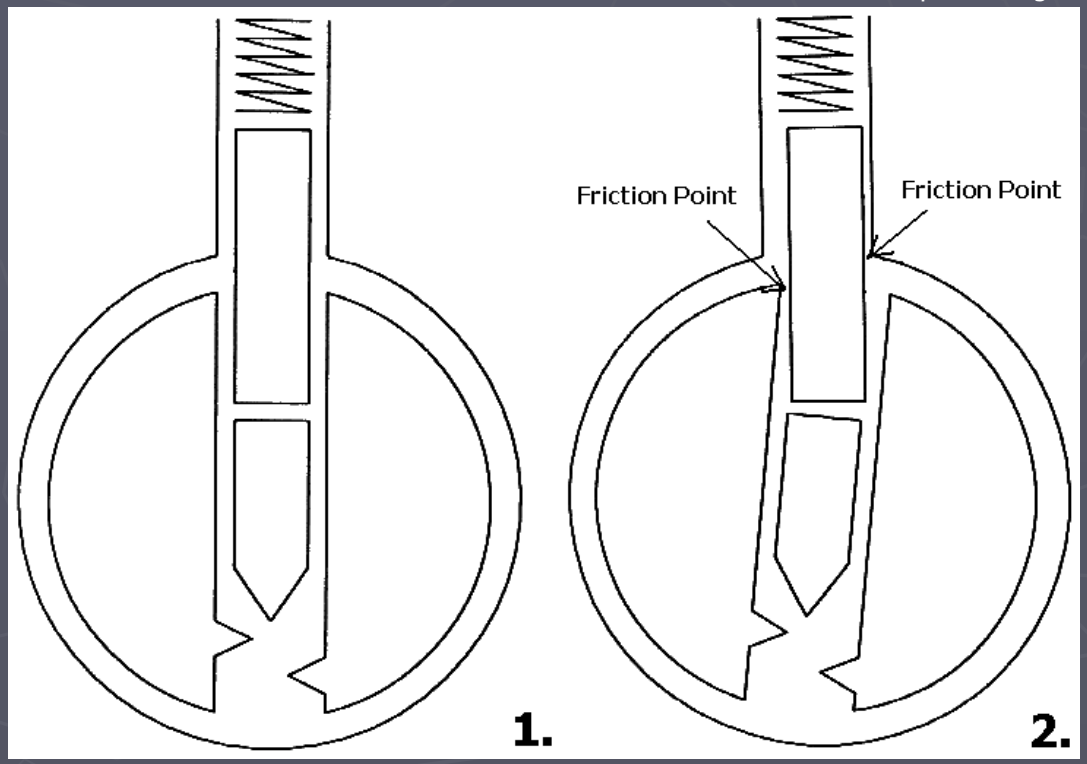
1. Because most locks are not built absolutely perfect, when applying torque to the lock, attempt to feel around the pistons with a little jab of the pick to best determine which binds first. By doing this you have the best chance of finding a pin that will sit nicely on the plug (shear line).
2. By moving from pin to pin working on the pins that bind the most first, hopefully you will be able to press all of the upper pins out of the plug and into the pistons. When you have done this, the torque you are applying to the lock will allow you to turn it. Voila, its open!
3. Remember that this a delicate art that requires a great deal of practice. Over time a trained locksmith will acquire a feeling for the pins that are in specific locks. It is all about feel.

Time for a little mathematics…

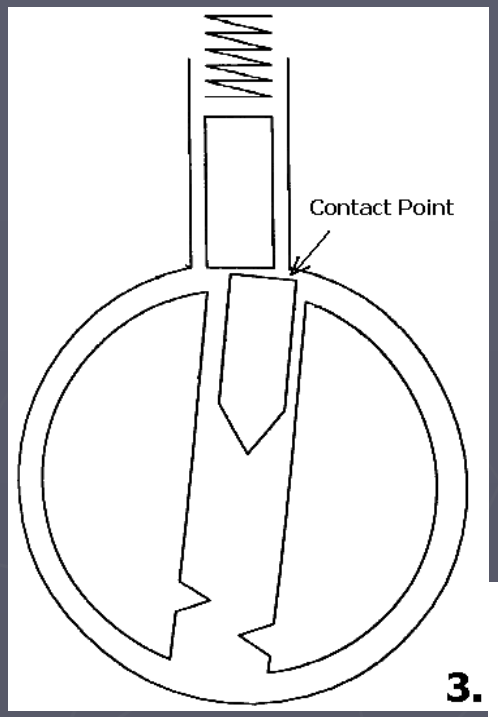
Here we look at the amount of force necessary to press the lower pin upward with a pick. We will see how the amount of force changes as the pins are pressed up the plug into the hull.

1. If a force is applied to the bottom of the lower pin the only resistance seen will be the spring force.
2. As the plug is torqued, and a force is applied to the bottom pin, there will be friction as the upper pin meets and binds against the hull.

Taken and modified from www.capricorn.org

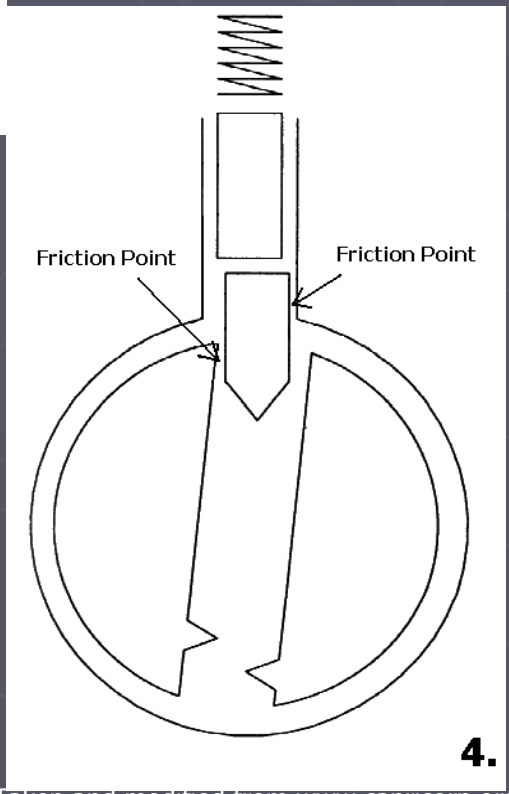


1. As the bottom pin is pressed further (in turn sliding the upper pin upwards) it will eventually reach the sheer line. At this point resistance will almost entirely disappear (only spring force) and the plug will turn ever so slightly. Shortly thereafter a contact force will be created as the bottom pin jabs into the hull. This causes a peak in the amount of force needed to move the pin.



3.

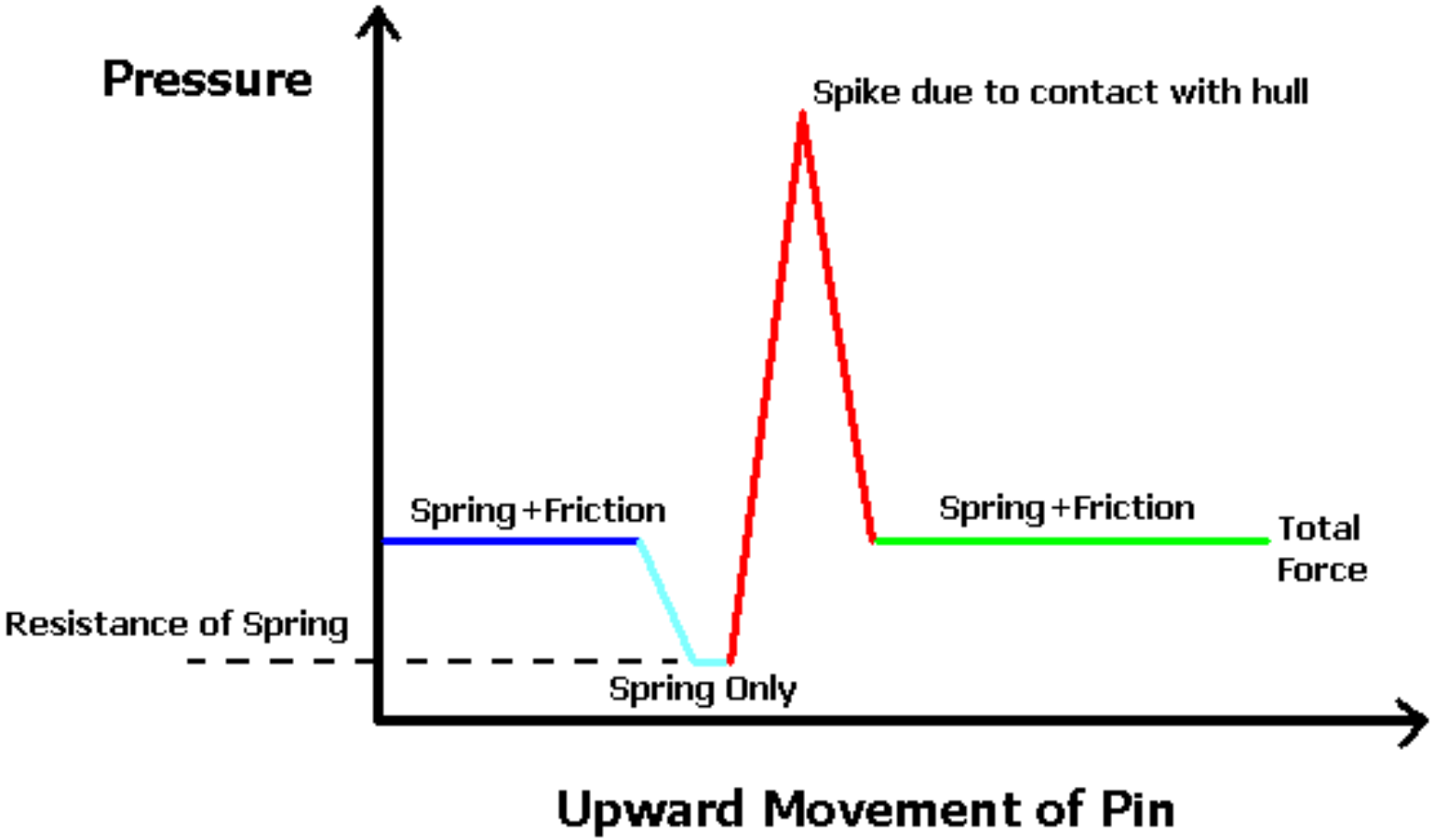
1. Once this resistance peak is passed the bottom pin enters the piston. At this point, two new friction points are established as the lower pin binds between the plug and the hull. Sound familiar? Here the lower pin is creating the same resistance the upper pin did in figure #1.



4.

Taken and modified from www.capricorn.org

Graphical Representation of Resistance



Less Scientific Method of Lock Picking

Raking or Scrubbing

A quicker method to lock picking is something known as scrubbing, or raking. This procedure is useful in situations where you do not have the luxury of taking your sweet time picking individual pins.

This method involves applying torque to the plug just as the standard method does. But instead of picking individual pins, you take a fairly wide tipped pick to the back of the plug. You pull it out while applying an upward force on the pins greater than the spring and friction force, but not greater than the collision force. You repeat this process multiple times until the lock turns.

The idea is that each raking of the pins will cause a few of the upper pins to land upon the shear line. Repeating this will eventually result in all of the pins resting on the plug and the lock being picked.

For more info on lock picking…

If you'd like to learn more about lock picking here is some helpful literature to look out for:

- Visual Guide to Lock Picking by Mark McCloud
- Secrets of Lock Picking by Stephen Hampton
- Modern High Security Locks: How to open them by Stephen Hampton
- Complete Guide to Lock Picking by Eddie the Wire